Amendment to the Claims:

1. (Currently Amended) A method of secret key agreement between a first [[(16)]] and a second [[(18)]] correspondent, the method comprising the acts of:

(a) said first correspondent receiving a response A, from a source P [[(20)]], said first correspondent comprising a first arithmetic logic unit;

(b) said second correspondent receiving a response B from said source P [[(20)]], said second correspondent comprising a second arithmetic logic unit;

(c) said first correspondent generating (d-1) parity symbols as an output of a codeword W whose input includes said response A and a secret key K selected by said first correspondent [[(16)]];

(d) said first correspondent [[(16)]] transmitting said (d-1) parity symbols over a public communication channel [[(22)]] to said second correspondent [[(18)]]; and

(e) said second correspondent [[(18)]] generating a [[word]] codeword W' whose input includes said (d-1) parity symbols and said response B to determine said secret key K;

wherein the secret key K may be determined from said (d-1) parity symbols and said response B by satisfying an inequality,

$$dH(A,B) <= (d - 1 - k) / 2$$

where

dH(A,B) is a Hamming distance between symbol sequences A and B,

d is a minimum distance, and

k is a number of symbols in the secret key K.

2. (Currently Amended) The method of Claim 1, wherein said responses A and B are received by said respective first [[(16)]] and second [[(18)]] correspondents responsive to a challenge C generated from said respective first [[(16)]] and second [[(18)]] correspondents.

3. (Original) The method of Claim 1, wherein said response A is comprised of a sequence of symbols of the form A=(a1,......an).

4. (Original) The method of Claim 1, wherein said response B is comprised of a sequence of symbols of the form B=(b1,……,bn).

5. (Original) The method of Claim 1, wherein said secret key K is comprised of a sequence of symbols of the form K=(k1,……,kk).

6. (Cancelled)

7. (Currently Amended) The method of Claim 1, wherein the codeword W'_ is a Reed-Solomon codeword.

8. (Currently Amended) The method of Claim 1, wherein the secret key K cannot be determined by someone other than said first and second correspondent [[(18)]] if the following inequality is satisfied,

dH(A,E) >= d-1

where:

E is a symbol sequence obtained by an attacker [[(17)]] attempting to learn the secret key K,

dH(A,E) is [[the]] a Hamming distance between the symbol sequences A and E.[[, and]]

~~d is the minimum distance.~~

9. (Currently Amended) A method of secret key agreement between a first and a second correspondent [[(18)]], the method comprising the acts of:

during an enrollment phase:

(a) sending to a source [[(20)]], a challenge C, from a first correspondent [[(16)]] at a time t1, wherein said first correspondent is a first computer;

(b) said first correspondent [[(16)]] receiving said response A to said challenge C;

(c) sending to said source [[(20)]], said challenge, from said second correspondent [[(18)]] B at a time t2, wherein said second correspondent is a second computer;

(d) said second correspondent [[(18)]] receiving a response B to said challenge C.

during an encoding phase, said first correspondent [[(16)]]:

(a) selecting a secret key K;

(b) forming a codeword W using said secret key K and said response A to generate (d-1) parity symbols P;

(c) transmitting said (d-1) parity symbols P to said second correspondent (18) over a public communication channel;

during a decoding phase, said second correspondent [[(18)]]:

(a) using said d-1 transmitted parity symbols and said response B to construct a [[word]] codeword W' to determine the secret key K if said response A and response B match within a selected tolerance;

wherein d is a minimum distance for correcting erasures and errors to provide said second correspondent with an ability to determine the secret key K transmitted from said first correspondent.

10. (Original) The method of Claim 9, wherein said response A is comprised of a sequence of symbols of the form A=(a1,......an).

11. (Original) The method of Claim 9, wherein said response B is comprised of a sequence of symbols of the form B=(b1,......,bn).

12. (Original) The method of Claim 9, wherein said secret key K is comprised of a sequence of symbols of the form K=(k1,......,kk).

13. (Currently Amended) The method of Claim 9, wherein the secret key K may be determined from said [[word]] codeword W' if and only if [[the]] an inequality is satisfied

$$dH(A,B) <= (d - 1 - k) / 2$$

where dH(A,B) is [[the]] a Hamming distance between symbol sequences A and B,

d is the minimum distance, and

k is [[the]] a number of symbols in the secret key K.

14. (Currently Amended) The method of Claim 9, wherein the codeword W'_ is a Reed-Solomon codeword.

15. (Currently Amended) The method of Claim 9, wherein the secret key K cannot be determined from someone other than said first and second correspondent [[(18)]] if and only if the following inequality is satisfied:

dH(A,E) >= d-1

where

E is a symbol sequence obtained by an attacker [[(17)]] attempting to learn the secret key K,

dH(A,E) is [[the]] <u>a</u> Hamming distance between the symbol sequences A and E.[[, and]]

~~d is the minimum distance.~~

16. (Currently Amended) A method of secret key agreement between a first and a second correspondent [[(18)]], the method comprising the acts of:

said first correspondent [[(16)]] receiving a response A from a source P [[(20)]];

said second correspondent [[(18)]] receiving a response B from said source P [[(20)]];

said first correspondent [[(16)]] generating (d-1) parity symbols as an output of a codeword W whose input includes said response A and a secret key K selected by said first correspondent [[(16)]];

said first correspondent [[(16)]] transmitting said (d-1) parity symbols and a pseudo-random function evaluated in A, over a public communication channel to said second correspondent [[(18)]]; and

said second correspondent [[(18)]] generating a [[word]] <u>codeword</u> W' whose input includes said (d-1) parity symbols, said pseudo-random function evaluated A, and said response B, to determine said secret key K selected by said first correspondent [[(16)]] <u>if said response B matches response A within a minimum distance for correcting erasures and errors;</u>

<u>wherein d is the minimum distance for correcting erasures and errors to provide said second correspondent a ability to determine the secret key K; and</u>

<u>wherein said first and second correspondents include computers.</u>

17. (Currently Amended) The method of Claim 16, wherein the pseudo-random function is a hash function of the form h(A)=(h(a1),...,h(an)), where A is the response A from said source P [[(20)]].

18. (Original) The method of Claim 16, wherein said response A is comprised of a sequence of symbols of the form A=(a1,......an).

19. (Original) The method of Claim 16, wherein said response B is comprised of a sequence of symbols of the form B=(b1,......,bn).

20. (Original) The method of Claim 16, wherein said secret key K is comprised of a sequence of symbols of the form K=(k1,......,kk).

21. (Currently Amended) The method of Claim 16, wherein the secret key K may be determined from said [[word]] <u>codeword</u> W' if the inequality is satisfied,

$$dH(A,B) <= (d - 1 - k)$$

where

dH(A,B) is [[the]] <u>a</u> Hamming distance between symbol sequences A and B,

~~d is the minimum distance,~~ and

k is [[the]] <u>a</u> number of symbols in the secret key K.

22. (Currently Amended) The method of Claim 16, wherein the codeword W<u>'</u> is a Reed-Solomon codeword.

23. (Currently Amended) The method of Claim 16, wherein the secret key K cannot be determined from someone other than said first and second correspondent<u>s</u> [[(18)s]] if the following inequality is satisfied:

$$dH(A,E) >= d\text{-}1$$

where

E is an attacker [[(17)]] attempting to learn the secret key K,

dH(A,E) is [[the]] a Hamming distance between the symbol sequences A and E, and

d is the minimum distance.

24. (Currently Amended) A method of secret key agreement between a first and a second correspondent [[(18)]], the method comprising the acts of:

during an enrollment phase:

sending to a source [[(20)]], a challenge C, from said first correspondent [[(16)]] at a time t1, wherein said first correspondent is a first arithmetic logic unit;

receiving said response A to said challenge C;

sending to said source [[(20)]], said challenge C, from said second correspondent [[(18)]] at a time t2, wherein said second correspondent is a second arithmetic logic unit;

during an encoding phase:

said first correspondent [[(16)]] selecting a secret key K;

forming a codeword W using said secret key K, a response A received by said first correspondent [[(16)]] during an enrollment phase and d-1 parity symbols P;

transmitting said d-1 parity symbols P and h(A) a pseudo-random function of A from said first correspondent [[(16)]] to said second correspondent [[(18)]] over a public communication channel;

during a decoding phase:

using said d-1 transmitted parity symbols and said pseudo-random function evaluated in A by said second correspondent [[(18)]] to construct a [[word]] codeword W' to determine the secret key K if said response A matches response B match sufficiently;

wherein d is a minimum distance for correcting erasures and errors to provide said second correspondent with a ability to determine the secret key K transmitted from said first correspondent.

25. (Original) The method of Claim 24, wherein the pseudo-random function is a hash function h(A)=(h(a_1),…,h(a_n))

26. (Original) The method of Claim 24, wherein said response A is comprised of a sequence of symbols of the form A=(a1,......an).

27. (Original) The method of Claim 24, wherein said response B is comprised of a sequence of symbols of the form B=(b1,......,bn).

28. (Original) The method of Claim 24, wherein said secret key K is comprised of a sequence of symbols of the form K=(k1,......,kk).

29. (Currently Amended) The method of Claim 24, wherein the secret key K may be determined from said [[word]] codeword W' if the inequality is satisfied,

$$dH(A,B) <= (d - 1 - k)$$

where

dH(A,B) is [[the]] a Hamming distance between symbol sequences A and B,

~~d is the minimum distance,~~ and

k is [[the]] a number of symbols in the secret key K.

30. (Currently Amended) The method of Claim 24, wherein the codeword W' is a Reed-Solomon codeword.

31. (Currently Amended) The method of Claim 24, wherein the secret key K cannot be determined from someone other than said first and second correspondents [[(16,18)]] if the following inequality is satisfied:

$$dH(A,E) >= d-1$$

where

E is a symbol sequence obtained by an attacker [[(17)]] attempting to learn the secret key K,

dH(A,E) is [[the]] a Hamming distance between the symbol sequences A and E.[[, and]]

~~d is the minimum distance.~~

32. (Currently Amended) A method of secret key agreement between a first and a second correspondent [[(18)]], the method comprising the acts of:

said first correspondent [[(16)]] receiving a response A from a source P [[(20)]], where A is a set of symbols, said first correspondent being a first computer;

said second correspondent [[(18)]] receiving a response B from said source P [[(20)]], where B is a set of symbols, said second correspondent being a second computer;

said first correspondent [[(16)]] ordering the set of symbols A into a sequence, a1,......,aN;

said first correspondent [[(16)]] computing a pseudo-random function of the ordered set of symbols A, h(A);

said first correspondent [[(16)]] transmitting h(A)=(h(a1),...h([[an]]a_j)),where j = 1....n, to said second correspondent [[(18)]]; and;

said second correspondent [[(18)]] computing a pseudo-random function of the ordered set of symbols B, h([[b]]b_j), where j = 1....n, for each symbol [[b]] in the set B;

said second correspondent [[(18)]] computing a set S which includes all positions j for which there exists an element in B such that h([[aj]] a_j) = h([[b]] b_j);

said second correspondent [[(18)]] transmitting the set S back to said first correspondent [[(16)]]; and

both first and second correspondents [[(16, 18)]] extracting a joint key J based on the symbols aj, j in S and for those symbols b in set B for which h([[aj]] a_j) = h([[b]] b_j).

33. (Original) The method of Claim 32, further comprising the act of extracting a secret key K from said joint key J using privacy amplification.

34. (Original) The method of Claim 33, wherein using said privacy amplification includes using one of a random matrix multiplier for multiplication with the joint key J and the joint key J evaluated in a hash function.

35. (Currently Amended) The method of Claim 32, wherein said responses A and B are received by said respective first [[(16)]] and second [[(18)]]

correspondents responsive to a challenge C generated from said respective first [[(16)]] and second [[(18)]] correspondents.

36. (Currently Amended) The method of Claim 32, wherein said response A is comprised of a sequence of symbols of the form A=(a1,......[[an]]$\underline{a_j}$).

37. (Currently Amended) The method of Claim 32, wherein said response B is comprised of a sequence of symbols of the form B=(b1,......,[[bn]]$\underline{b_j}$).

38. (Original) The method of Claim 32, wherein said secret key K is comprised of a sequence of symbols of the form K=(k1,......,kk).